



U.S. Department of Justice

Federal Bureau of Investigation

DOCKET FILE COPY ORIGINAL

Telecommunications Industry Liaison Unit
P.O. Box 220450
Chantilly, VA 20153-0450

December 12, 1997

By Hand Delivery

Ms. Magalie R. Salas, Secretary
Federal Communications Commission
1919 M Street, N.W., Room 222
Washington, D.C. 20554


Re: *In the Matter of Communications Assistance for Law Enforcement Act*, CC
Docket No. 97-213 (released October 10, 1997)

Dear Ms. Salas:

Enclosed for filing in the above-referenced proceeding are an original and eleven (12) copies of the Comments of the Federal Bureau of Investigation and Law Enforcement regarding the implementation of the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.), and an accompanying Certificate of Service.

An additional copy of comments is enclosed to be stamped "received" and returned.

Thank you very much for your attention to this matter.

Sincerely,

Rozanne R. Worrell
Supervisory Special Agent
Federal Bureau of Investigation

Enclosure

No. of Copies rec'd
List ABCDE

043

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of:

Communications Assistance for Law
Enforcement Act

)
)
) CC Docket No. 97-213
)
)
_____)

To: The Commission

**COMMENTS OF
THE FEDERAL BUREAU OF INVESTIGATION
REGARDING IMPLEMENTATION OF THE
COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT**

Dated: December 12, 1997

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND	2
III.	LEGISLATIVE HISTORY	7
IV.	DEFINITION OF TELECOMMUNICATIONS CARRIER	11
V.	CARRIER SECURITY POLICIES AND PROCEDURES	15
A.	The Commission Should Make It Clear That Carriers' Duty Under CALEA to Ensure That Intercepts Are Appropriately Executed Applies to Its Personnel Designations, Employee Oversight, and Personnel Practices and Procedures	15
B.	The Commission Should Require Carrier Procedures That Ensure the Timeliness, Security, and Integrity of Electronic Surveillance Conducted on Law Enforcement's Behalf	18
1.	Personnel Procedures	18
2.	Reports of Violations	20
C.	The Commission Should Specify That Carriers Are Not Required to Review the Substantive Basis or Underlying Legal Authority for Facially Valid Intercept Requests	22
D.	The Commission Should Ensure That Internal Carrier Authorizations and Procedures Are Designed to Maintain the Timeliness, Security, and Accuracy of Intercepts	24
1.	Designated Personnel	24
2.	Intercept Authorizations	27
3.	Record Keeping	29
4.	Timeliness	30
E.	No Distinction Is Made for Small Carriers Under CALEA.	32
F.	Commission Procedures	35
VI.	JOINT BOARD	36
VII.	ADOPTING TECHNICAL STANDARDS.....	36

VIII.	REQUESTS UNDER THE REASONABLY ACHIEVABLE STANDARD	38
IX.	EXTENSIONS OF COMPLIANCE DATE	41
X.	REPORTING AND RECORD KEEPING	42
XI.	CONCLUSION	42

**Before the
Federal Communications Commission
Washington, DC 20554**

In the Matter of:)

Communications Assistance for Law)
Enforcement Act)
_____)

CC Docket No. 97-213

**Comments of the Federal Bureau of Investigation
Regarding Implementation of the Communications
Assistance for Law Enforcement Act (CALEA)**

I. INTRODUCTION

1. The Federal Bureau of Investigation (FBI), by its attorneys, respectfully submits its comments in the above-referenced proceeding on its own behalf and on behalf of other Federal, state, and local law enforcement agencies (hereinafter referred to collectively as "Law Enforcement").¹ The Communications Assistance for Law Enforcement Act (CALEA)² assigns a set of roles and responsibilities to the telecommunications industry, law

¹ Following the enactment of CALEA, the FBI assembled the Law Enforcement Technical Forum ("LETf"), which consists of representatives from 21 Federal and 30 state and local law enforcement agencies, as well as the Royal Canadian Mounted Police. LETf members have participated in the development of the positions submitted with these comments. In turn, the FBI and the LETf have coordinated CALEA implementation issues, and developed consensus positions, with several hundred of the major law enforcement agencies and prosecutors' offices across the United States.

² Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in sections of 18 U.S.C. and 47 U.S.C.). The purpose of CALEA is to preserve electronic surveillance capabilities authorized by Federal and state law. The Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1801-*et seq.*, authorizes the government to conduct electronic surveillance for intelligence purposes. However, because of the classified and sensitive nature of electronic surveillance conducted under FISA, the FBI will, hereinafter, focus its comments upon criminal law-based electronic surveillance authority and activity. These comments are not intended to apply to those additional classified issues raised under FISA.

The Commission and telecommunications carriers should recognize, however, that nothing in CALEA, or the regulations to be promulgated in this proceeding, relieves carriers of their obligations to provide all necessary assistance to law enforcement under FISA, as set forth at 50 U.S.C. § 1805(b)(2)(B). While the techniques used for electronic surveillance collection under FISA are essentially the same as under

enforcement, the Federal Communications Commission (FCC), and other governmental agencies in the implementation of the various regulatory requirements and other mandates under the statute. This proceeding was implemented to deal specifically with those roles assigned by Congress to the Commission. Law Enforcement welcomes and is pleased to participate in the Commission's effort.

II. BACKGROUND

2. Historically, law enforcement officers, after securing a lawful electronic surveillance order³ would serve a secondary "assistance order" on the affected carrier to obtain relevant line and appearance information and leased line delivery circuits.⁴ Moreover, in most cases, after serving the assistance order on the carrier, law enforcement technical agents were able to effect the authorized intercept themselves at locations in the "local loop," removed from the carrier's central office or switch. Such local loop-based

criminal law-based Federal electronic surveillance authority and activity, there are legally specified administrative procedures regarding the handling of classified electronic surveillance orders and materials. These administrative procedures are most appropriately addressed directly by the FBI with telecommunications carriers on an as needed basis pursuant to Executive Order 12958. Moreover, the FBI believes that the Commission will appreciate the problematic nature of a regulatory body's inclusion of classified matters in a broad-based rulemaking effort such as the instant one.

³ Federal electronic surveillance orders may be issued pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, 18 U.S.C. §§ 2510-2522 (referred to herein as "Title III"). Title III electronic surveillance orders pertain to the content of communications. Orders for the use of pen register and trap and trace devices, which provide call-identifying information, are issued pursuant to 18 U.S.C. §§ 3121-3127. Electronic surveillance and pen register and trap and trace orders may also be issued pursuant to state electronic surveillance statutes. Throughout these comments, "electronic surveillance," "interception," and "intercept" are used interchangeably to refer to electronic surveillance activities.

⁴ Aside from including law enforcement's electronic surveillance search authorities, both the Federal Title III and the pen register and trap and trace statutes (as well as most state statutes) contain long-standing statutory provisions mandating that telecommunications service providers and others shall furnish the applying law enforcement agency "forthwith *all* information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services...[accorded] the person whose communications are to be intercepted" (emphasis added). Law enforcement is also required under this pre-CALEA, Title III provision to compensate the carrier for reasonable expenses incurred in providing such facilities or assistance. 18 U.S.C. § 2518(4). Analogous provisions exist with regard to pen register and trap and trace efforts. 18 U.S.C. § 3124. (FISA -based assistance provisions are found at 50 U.S.C. § 1805(b)(2)(B)).

interceptions, which historically dealt with ordinary, two-party, plain old telephone service (POTS) communications, were highly effective and successful. Thus, in the past, law enforcement was able to intercept *all* of the communications content and call identifying information supported by a subject-subscriber's POTS telephone service.

3. In addition, in the past, there were fewer carriers within a region, and those carriers' security personnel, as a general rule, were easy to ascertain and contact. As a result, in most cases, law enforcement was readily able to determine the identity of the relevant carrier and generally able to obtain the necessary assistance without unreasonable delays. Today, the proliferation of carriers and increasing centralization of their security functions have made it considerably more difficult, from both a procedural and practical point of view, for law enforcement to conduct, or effect, electronic surveillance. Larger carriers also have tended to concentrate their security functions in a single office within the carrier's entire region, which complicates both the installation of the intercept and the delivery of surveillance information. For example, if a law enforcement officer in Bell Atlantic's New Jersey territory obtains a court order for electronic surveillance on a subject subscriber's telephone in New Jersey, he must contact the Bell Atlantic security office in Virginia. As a result, a number of carrier personnel and facilities can be involved in implementing an intercept, which, if not properly addressed, can add delay to the process.

4. Moreover, internal administrative procedures employed by telecommunications carriers tend to vary from carrier to carrier. The level of scrutiny applied to judicial orders in some instances is overly extensive. Indeed, review by carrier personnel has resulted in facially valid intercept orders being inappropriately delayed, frustrated, or rejected.

5. Further, in recent years, rapid advances in technology, such as the deployment of new switch- and network-based services and features and the dispersion of intelligence throughout carrier networks, have eroded law enforcement technical agents' ability to fully

and properly effect intercepts themselves. It is becoming apparent that surveillance solutions must increasingly become switch- and network-based.

6. It is well known that advanced telecommunications technology has changed the way telephone calls are established, processed, and maintained. As stated above, telecommunications frequently are no longer the two-party POTS calls of the past; multiparty calls having several different "legs" have become common. Second, calls no longer rely on dialed digits as the exclusive means of processing, establishing, and maintaining such calls; other signaling is centrally involved. Third, with the advent of subscriber-initiated multiparty calls, law enforcement is able to intercept only *part* of the communications being supported by the subject-subscriber's telephone service (i.e., those occurring over the leg of the call that the subject-subscriber's terminal equipment is actually connected to at any point in time). Fourth, subscribers are being offered calling features and services (e.g., conference calling, call forwarding) that can rapidly change almost instantaneously the nature of the subscriber's service, which, in turn, could lead to insufficient acquisition of interception delivery channels and circuits by law enforcement.⁵ For all these reasons, therefore, law enforcement has been technologically impeded from intercepting all of the lawfully authorized communications content and call-identifying information connected with, and supported by, the subject-subscriber's telephone service.

7. Nevertheless, even though the telecommunications markets in which lawful intercepts are effected have changed dramatically, law enforcement's primary electronic surveillance concerns have not changed. These concerns are the timeliness, security, accuracy, and evidentiary integrity of all lawful electronic surveillance. The public safety

⁵ Although law enforcement agencies check with telecommunications carriers before a Title III or pen register effort begins, absent a message advising law enforcement of new services, there could be significant delay in effecting added delivery channels. As a result, without adequate delivery circuits, a substantial amount of the intercepted information will go undelivered—figuratively "falling on the floor."

and the criminal prosecutions that necessitate electronic surveillance depend for their success on strict attention to these concerns.

8. Generally, the longer it takes to effect an intercept order, the greater the possibility that critical evidence and information will be lost because a criminal subject has moved on or because the intercept order has expired.⁶ The more carrier personnel involved in effecting an intercept, the more likely it is that the security of a particular surveillance may be compromised. Delays in reporting a technical or human compromise of an intercept, for example, may result in subjects becoming apprised that surveillance exists without law enforcement's knowledge of that compromise. In such a case, not only will the evidentiary value of the electronic surveillance be eroded, but the safety of undercover law enforcement officers or the intercept subjects may be endangered. Delays or flaws in a carrier's operational procedures for responding to surveillance orders can also threaten the accuracy and integrity of electronic surveillance.⁷

9. All of these issues bear generally on the evidentiary integrity of electronic surveillance information and could conceivably present a basis upon which to challenge the admissibility of evidence.⁸ For this reason, Law Enforcement believes that the Commission's rules establishing carrier policies and procedures are a critically important piece of the CALEA implementation process. It would be in the best interests of the carriers charged with responding to law enforcement's valid electronic surveillance orders to

⁶ No Title III order is valid for more than 30 days, with the 30 days beginning to run on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or 10 days after the order is entered. 18 U.S.C. §2518(5).

⁷ If an intercept subject changes his service or subscribes to a new feature offered by a carrier that enables him to reroute his communications, the law enforcement electronic surveillance effort may be bypassed, and important evidence lost, for an extended period before law enforcement becomes apprized.

⁸ Since, under CALEA, the implementation of electronic surveillance orders will increasingly shift to telecommunications carriers, Law Enforcement's electronic surveillance activity could be rendered ineffectual if the evidence that results from lawful intercepts is subjected to court challenge based on lax carrier procedures.

implement policies and procedures that safeguard and promote the timeliness, security, integrity, and accuracy of electronic surveillance activity.

10. Among the key issues addressed by CALEA are the telecommunications entities covered by the statute and the obligations these entities must meet to ensure they will be able to comply with electronic surveillance orders. Further, as telecommunications technology evolves and new services and capabilities are introduced into the market, the Commission's role in evaluating whether, and how, CALEA's obligations will extend to new services or providers will become increasingly important. Indeed, in the future, as telecommunications markets continue to grow and become more competitive, telecommunications providers are likely to become more differentiated in the range of services they offer.

11. Concepts such as number and service portability, as well as other advances in technology, likely will enable consumers to pick from a much broader range of services offered by multiple providers.⁹ Indeed, as digitization, packet switching, bandwidth conservation methods, and innovative network management and switching techniques continue to redefine the traditional understanding of "telecommunications," the Commission will be asked to play a critical public safety role in ensuring that law enforcement can continue to fully and properly conduct lawful electronic surveillance.

12. For these reasons, Law Enforcement welcomes the Commission's efforts to address the issues raised by the mandates contained in CALEA, particularly those regarding the definition of telecommunications carrier and carrier systems security and integrity policies and procedures. The rules to be developed by the Commission with respect to these definitions and carrier policies and procedures will have a direct impact on Law

⁹ See generally 47 U.S.C. § 153(30); *Telephone Number Portability*, [Second Report And Order], CC Docket No. 95-116; 12 FCC Rcd 12281 (released August 18, 1997); and *Telephone Number Portability* [First Report And Order], CC Docket No. 95-116; 11 FCC Rcd 8352 (released July 2, 1996) (discussions of number and service portability).

Enforcement's future conduct of its investigative and evidentiary collection activities with respect to electronic surveillance. As such, although Law Enforcement recognizes the need to not unduly burden the administration of internal carrier systems and procedures, it is equally important that the Commission craft rules, procedures, and policies that will accommodate Law Enforcement's investigative efforts and public safety demands. An understanding of CALEA's legislative history may be helpful to the Commission's consideration of these issues.

III. LEGISLATIVE HISTORY

13. Congress passed CALEA and President Clinton signed it into law in October 1994. As the legislative history articulates, CALEA was passed "to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services."¹⁰

14. Passage of CALEA was not without precedent; it was a logical and necessary development of the Nation's electronic surveillance laws. Congress' enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 served as the foundation for defining communications privacy and law enforcement electronic surveillance authority. Subsequently, as telecommunications technology continued to change, Congress passed the

¹⁰ H.R. Rep. No. 827, 103rd Cong., 2d Sess., 9, *reprinted in* 1994 U.S. Code Cong. & Ad. News 3489 (1994). It is important to note that the final version of CALEA was substantially rewritten by subcommittees of the House and Senate Commerce Committees. The House Report accompanied an earlier version of CALEA, sponsored by the Judiciary Committee. There are no Commerce Committee reports.

Electronic Communications Privacy Act of 1986, which extended law enforcement intercept authority to new technologies and services, such as electronic mail, cellular telephones, and paging devices.¹¹

15. However, telecommunications technology continued to change at an even more rapid pace in the years following 1986. This technological change resulted in unique challenges for law enforcement. FBI Director Louis J. Freeh, speaking on behalf of other Federal, state, and local law enforcement communities, expressed the effect of these changes on law enforcement when he testified before Congress in March and August 1994.¹² In his remarks – the first in a series of hearings on “Digital Telephony” – Director Freeh testified that a variety of advanced telecommunications services and features were eroding law enforcement’s ability to enforce the law through the use of the authorities set forth in the Federal and state electronic surveillance laws and related pen register and trap and trace statutes.

16. Director Freeh testified that without remedial legislation “one of the most effective weapons against national and international drug trafficking, terrorism, espionage, organized crime, and serious violent crimes [would] be severely and adversely impacted.”¹³ He stated, “The indisputable fact is that emerging and future technology will have a much greater and more devastating impact on law enforcement and the public safety unless

¹¹ See 18 U.S.C. §§ 2510-*et seq.*; 18 U.S.C. §§ 2701-*et seq.*; and 18 U.S.C. §§ 3121-*et seq.* See also H.R. Rep No. 103-827, at 12.

¹² *Joint Hearing on the Proposed Legislation, “Digital Telephony and Communications Privacy Improvement Act of 1994,”* Before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, 103rd Cong., 2d Sess. (Mar. 18, 1994) (hereinafter *Director Freeh’s Statement*).

¹³ Director Freeh’s Statement at 2.

Congress acts now to ensure that current impediments are removed and new ones are not introduced.”¹⁴

17. Director Freeh stated that the purpose of the proposed legislation was “. . . to maintain technological capabilities *commensurate with existing statutory authority*—that is, to prevent advanced telecommunications technology from repealing *de facto* statutory authority already conferred by Congress” (emphasis added).¹⁵ Director Freeh emphasized that the legislation “. . . deals with the advanced telephony problem *in an appropriately comprehensive fashion*—it does not simply ‘band-aid-over’ past problems; it also responsibly deals with new services and technologies (such as personal communications services) that likely will emerge. . . [o]n the other hand, the legislation is narrowly focused on where the vast majority of the problems exist—the networks of common carriers, a segment of the industry which historically has been subject to regulation” (emphasis added).¹⁶ It clearly was not intended to preserve or maintain past ineffective electronic surveillance capabilities that were no longer working fully or properly.

18. Thus, in analyzing CALEA, it is important to recognize that Congress clearly understood the essence of CALEA to be the *comprehensive preservation and maintenance of electronic surveillance and related statutory search authority* granted to law enforcement

¹⁴ Director Freeh’s Summary Statement (Summary Statement of the full statement referred to in note 12) at 10.

¹⁵ Director Freeh’s Statement at 2-3.

¹⁶ Director Freeh’s Statement at 3-4.

agencies by law. These goals are to be achieved through whatever technical modifications are necessary.¹⁷

19. When Congress passed CALEA in October 1994, it heeded Director Freeh's request to maintain court-authorized or otherwise approved electronic surveillance. Congress required that CALEA ensure that new technologies and services will not hinder law enforcement access to the communications content and call-identifying information occurring over the telecommunications service that is the subject of a court order authorizing electronic surveillance. At the same time, Congress sought to balance law enforcement's needs with the privacy interests of the American public and with the telecommunications industry's need to develop and deploy new services and technologies that benefit society. As the House Report states: "[t]he bill seeks to balance three key policies: (1) to preserve a narrowly focused capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies."¹⁸ It is in this light that the Commission must exercise its mandate to implement those sections of CALEA over which it has jurisdiction.

¹⁷ In his Statement, Director Freeh advised, "Over the last decade, it is conservatively estimated that several hundred electronic surveillance and pen register and trap and trace court orders have been frustrated, in whole or in part, by various technological impediments. . . . It is important to note that there have been many instances where court orders have not been sought or served on carriers due to law enforcement's awareness of these pre-existing impediments . . ." *Director Freeh's Statement* at 32-33. Indeed, in 1994, the FBI provided the House and Senate Judiciary Committees with an illustrative list of 183 instances where the law enforcement agencies informally surveyed by the FBI stated that they had been impeded in conducting electronic surveillance-related efforts, in whole or in part, by advanced telecommunications services or features.

¹⁸ H.R. Rep. No. 103-827 at 13. Because of the extreme importance of fully effective electronic surveillance capability to public safety and effective law enforcement, Congress conferred authority on the Attorney General to enforce the assistance capability requirements set forth in CALEA Section 103 and conferred jurisdiction over such cases on the Federal courts. Moreover, to underscore the potential impact of this matter on public safety, civil penalties of up to \$10,000 per incident for each day in violation were included to ensure widespread carrier compliance with CALEA. See 18 U.S.C. § 2522.

IV. DEFINITION OF TELECOMMUNICATIONS CARRIER

20. Law Enforcement agrees that the Commission has drawn the correct conclusion that Section 601(c)(1) of the Telecommunications Act of 1996 (the "1996 Act") did not modify CALEA's definition of a "telecommunications carrier," or its definition of "information services." In addition, the 1996 Act by its own terms did not modify or supercede existing law, unless expressly so stated. The 1996 Act did not contain language indicating that it would modify the definitions of "telecommunications carrier" or "information service" for the purposes of interpreting CALEA.

21. Law Enforcement also agrees with the Commission's tentative conclusion that all entities defined as common carriers for purposes of the 1996 Act are telecommunications carriers subject to CALEA. Law enforcement also agrees with the Commission's determination that commercial mobile service providers fall within CALEA's definition of telecommunications carriers. In addition, Law Enforcement believes that any entity providing telecommunications services for hire to the public are subject to CALEA's requirements. This definition would include cable operators and electric and other utilities that provide telecommunications services for hire to the public.

22. Moreover, in the post 1996 Act environment, there may exist telecommunications companies that do not hold themselves out to serve the public indiscriminately that should also be treated as "telecommunications carriers" by the Commission.¹⁹ Otherwise, companies that hold themselves out to serve particular groups may, intentionally or inadvertently, undermine CALEA. Law Enforcement believes that if the Commission adopts the definition of telecommunications carrier as a company that holds itself out to serve the public indiscriminately, it may add a level of unnecessary ambiguity

¹⁹ See generally, P. Pitsch and A. Bresnahan, *Common Carrier Regulation of Telecommunications Contracts and the Private Carrier Alternative*, 48 Fed. Com. L.J. 447 (June 1996).

to its coverage. If the Commission were to adopt such language, it may create a loophole whereby criminals could use telecommunications service providers that do not indiscriminately offer their services to the public, thereby thwarting CALEA. Thus, the Commission should not incorporate the word "indiscriminately" into the definition of telecommunications carrier because it may cause an unnecessary ambiguity regarding the reach of the term "telecommunications carrier" under CALEA.

23. Finally, Law Enforcement agrees with the Commission's conclusion that providers of pay telephones are not telecommunications carriers for purposes of CALEA. Pay telephones, for purposes of CALEA, have more to do with end-user terminal equipment than with telecommunications services. It is Law Enforcement's contention that the type of terminal equipment being used for the telecommunications service is irrelevant under CALEA. CALEA is concerned with the type of telecommunications service, not the manufacturer or owner of the physical phone or device.

24. Law enforcement agrees with the Commission's proposal not to adopt a specific list of the types of carriers that would be subject to the obligations of CALEA because over time new communications technologies will come into existence. Law enforcement, however, is concerned that any type of illustrative list could be considered all-inclusive. Thus, Law Enforcement advocates that the Commission in its final rules state that any communication service, either wireline or wireless, for hire by the public, is subject to the obligations mandated by CALEA.²⁰ But, if the Commission believes that it is in the public interest to have an illustrative list of the types of entities that are subject to CALEA, Law Enforcement believes that it would be a useful clarification to specify that the following additional telecommunications services are included—

²⁰ The definition adopted by the Commission should make it clear that *any* service offered in this manner by a carrier would be subject to CALEA, including, for example, packet mode over digital subscriber lines ("DSL") services offered by carriers.

- Paging technologies
- Facility-based and switch-based resellers
- Specialized mobile services
- Enhanced specialized mobile services
- Aeronautical radio.

25. Law enforcement contends that paging systems should be included in the definition of “telecommunications carrier” for the purposes of interpreting CALEA because paging systems generally fall within the definition of common carrier or, at minimum, rely on common carriers to be activated. Individuals must call the paging service and then punch in their alphanumeric messages, such as phone numbers to call or messages. In addition, most common carriers for hire now provide phone systems that offer paging channel access. Thus, Law Enforcement advocates that the definition of telecommunications carrier, and any illustrative list the Commission may choose to create, should include pagers.

26. Further, Law Enforcement believes that resellers should be included in CALEA’s definition of telecommunications carrier. It is Law Enforcement’s contention that a reseller is accountable to assist Law Enforcement in any way technically feasible under CALEA. If the reseller is using any equipment or facilities for telecommunications service, the reseller and the incumbent owner of the telecommunications equipment or facility should be required to ensure that law enforcement officials will have access to their equipment or facilities for the purposes of electronic surveillance under CALEA. Law enforcement also contends that the definition of telecommunications carrier should include resellers with prepaid calling card or other similar services.

27. Law enforcement agrees with the Commission’s conclusion that CALEA affords the Commission the flexibility to classify new local exchange carriers and to include, as telecommunications carriers, entities that provide replacement for local exchange service but who otherwise do not fit neatly into the current definition of telecommunications carrier. In

the future, however, Law Enforcement will seek to consult with the Commission with regard to persons or entities offering services that become a replacement for local exchange service. Moreover, Law Enforcement agrees with the Commission's conclusion to decline to exercise its discretion at this time to include within the definition of telecommunications carrier specific persons or entities providing wire or electronic communication or switching service that is a replacement for a substantial portion of the local exchange service. The Commission should continually monitor new services and technologies because Law Enforcement believes that they could become a substantial replacement for local exchange service in the future.

28. Law enforcement recommends that the Commission not exercise its discretion pursuant to Section 102(8)(C)(ii) of CALEA, which allows the Commission to exclude specific classes or categories of carriers from the obligations of CALEA after consultation with the Attorney General. In this regard, only explicit exclusions of specific classes and categories of telecommunications carriers are sufficient to exempt carriers from their statutory obligations. In addition, Law Enforcement agrees with the Commission's tentative conclusion that private mobile service providers are not subject to the requirements of CALEA as long as the provider of private mobile service does not become a telecommunications service provider for hire by the public or replace a substantial portion of local exchange service. Once the private mobile service provider offers any portion of its services to the public for hire, or when such service offered on a private carriage basis substantially replaces any portion of the public switched network, it should be considered a telecommunications carrier as defined under CALEA.

29. Law enforcement agrees with the Commission's tentative conclusion that providers of exclusively information services are excluded from CALEA's requirements and are not required to modify or design their systems to comply with CALEA with regard to information services. Law Enforcement believes, however, that any portion of a telecommunications service provided by a common carrier that is used to provide transport

access to information services is subject to CALEA's requirements. Thus, Law Enforcement advocates that the Commission should consider a conservative definition of information services because of the possible criminal uses of such services.

30. Moreover, Law Enforcement agrees with the Commission's tentative conclusion that calling features associated with telephone service should be classified as telecommunications services under CALEA. Thus, telecommunications carriers offering these types of services must be required to make all necessary network modifications to comply with CALEA. In addition, Law Enforcement regards the Commission's list of calling features to be illustrative and not exclusive. Law Enforcement believes that any attempt by the Commission to make a comprehensive and exclusive list of calling features would be counterproductive and detrimental to law enforcement. An exclusive list would also be counterproductive because of the regulatory burden associated with updating the list each time a technological advancement occurs.

V. CARRIER SECURITY POLICIES AND PROCEDURES

A. The Commission Should Make It Clear That Carriers' Duty Under CALEA to Ensure That Intercepts Are Appropriately Executed Applies to Its Personnel Designations, Employee Oversight, and Personnel Practices and Procedures

31. Law Enforcement concurs with the Commission that carriers have an affirmative duty under CALEA to assist law enforcement in its duly authorized electronic surveillance activities. The underlying source of this duty is found, for example, in 18 U.S.C. Section 2518(4), which provides for intercept orders to require the provision by carriers of "all information, facilities, and technical assistance" necessary to accomplish the interception.²¹

²¹ Nearly identical assistance provisions are set forth in the pen register and trap and trace statutes. See 18 U.S.C. § 3124.

32. Law Enforcement also concurs with the Commission that the use of the word “authority” in Section 301 of CALEA (Section 229(b)(1) of the Communications Act of 1934) refers to the authority granted to a carrier’s employee by the carrier to engage in interception activity. By contrast, the first possible construction identified by the Commission in paragraph 25 of the Notice of Proposed Rulemaking (“NPRM”) would place carrier personnel in the position of reviewing the underlying validity and basis for a court order or, in the case of exigent circumstances, the authorization of a duly empowered law enforcement official.²² Law Enforcement strongly believes that carriers are not vested with such *de novo* review authority under CALEA or the electronic surveillance laws. Nor does Law Enforcement believe that CALEA grants discretion to the Commission to confer such authority on carriers.

33. Indeed, there have been anecdotal reports of instances where carriers have refused to provide assistance to law enforcement even after being presented with a facially valid court order in circumstances where carrier personnel “did not recognize” a particular judge’s signature or where the description of the carrier service to be included in the intercept did not precisely match the carrier’s brand name for that service. Yet it is clear from the assistance provisions in the electronic surveillance laws that it is not within the purview of carriers to look behind court orders or authorizations with the intention of enforcing the criminal law. The Commission has the opportunity, in furtherance of public safety, to establish rules in this proceeding that will minimize the likelihood of such case-by-case anomalies in the future.

34. To ensure that intercepts are conducted in a timely, secure, and accurate manner, the review that a carrier gives to a court order or certificate of authorization (provided in cases of exigent circumstances) should be limited to whether (1) the court order or

²² Law Enforcement agrees that carriers have a duty with regard to electronic surveillance effected within a carrier’s switching premises. However, not *all* future interceptions will be conducted at a carrier’s switching premise. There will continue to be instances where law enforcement elects to effect an intercept as it does currently: in the local loop, away from a carrier’s switching premises. Law enforcement’s service of process and conventional carrier assistance will continue for these local-loop-based activities.

certification is valid on its face (i.e., that it is what it purports to be); and (2) the intercept is capable of being implemented as a technical matter. Any further scrutiny by carrier personnel of the legal basis for the intercept would result in the judgment of a carrier's employee being substituted for the judgment of either the court (in the case of an order) or the law enforcement officer empowered to certify that exigent circumstances exist. Hence, the Commission should specify that the duty of the carrier upon receipt of a facially valid court order or statutorily-based authorization for an intercept extends only to the prompt and good faith implementation of such court orders or authorizations.

35. It has been argued that carriers may face potential civil or criminal liability if they implement a court order that later proves to be unlawful. It should be noted, however, that Section 105 of CALEA does not place any additional liability on carriers that does not already exist under common law or the provisions of applicable statutes (e.g., Title 18 of the United States Code). Indeed, the procedures under these existing criminal and civil statutes also provide avenues for responding to any abuse by law enforcement of its authority and discretion in cases of electronic surveillance. Moreover, Law Enforcement believes that the electronic surveillance laws make it clear that a carrier's good faith implementation of an intercept requested pursuant to a facially valid court order, or certification of exigent circumstances, all other things being equal, would provide the carrier a defense to claims of liability.²³ Of course, the good faith requirement might not be met in the event that unauthorized interceptions by carrier personnel resulted from a carrier's failure to exercise its duty to implement and enforce appropriate security policies and procedures.

²³ The duties imposed on carriers under Section 105 of CALEA do not expand the potential civil or criminal liability of carriers. Good faith reliance on a court order or a request of an investigative or law enforcement officer under 18 U.S.C. § 2518(7) is a complete defense to any civil or criminal action against a carrier. 18 U.S.C. § 2520(d)(1), (2). Further, in a criminal action, good faith reliance by a carrier would defeat the intent requirement of a *prima facie* case. Indeed, under 18 U.S.C. § 2511(2)(a), "no cause of action shall lie in any court" against a carrier providing information, facilities, or assistance in accordance with the terms of a court order or certificate of authorization. The same is true for derivative liability. *See also infra* note 24.

B. The Commission Should Require Carrier Procedures That Ensure the Timeliness, Security, and Integrity of Electronic Surveillance Conducted on Law Enforcement's Behalf

36. Law Enforcement strongly contends that any carrier activities that threaten to compromise the security of electronic surveillance activities could endanger lives and impede prosecutions. Thus, Law Enforcement agrees with the Commission's statement in Paragraph 26 of the NPRM that each carrier must ensure that the personnel it designates to implement and have access to interceptions perform only authorized interceptions, and that those personnel do not reveal the existence, or content, of those interceptions to anyone other than law enforcement personnel, except pursuant to valid court, legislative, or administrative order. The following comments are designed to ensure that carriers' personnel and administrative procedures regarding electronic surveillance include meaningful security protections.

1. Personnel Procedures.

37. Law Enforcement agrees with the Commission's statement in Paragraph 27 of the NPRM to the extent that civil liability may extend to a carrier under certain circumstances if its employees are found to have illegally intercepted communications.²⁴

²⁴ With respect to the Commission's statement concerning the extension of criminal liability, Law Enforcement believes that the risk of carrier liability is minimal. For a corporation to be convicted for the criminal act of its agent under a theory of *respondeat superior*, it must be found that the agent is acting within the scope of employment (i.e., the agent must be performing acts which he is authorized to perform for the corporation, and those acts must be motivated—at least in part—by an intent to benefit the corporation). See *U.S. v. Cincotta*, 689 F.2d 238, 241-42 (1st Cir. 1982). Law Enforcement believes that the duties imposed on carriers under Section 105 of CALEA do not add to a carrier's potential liability for criminal acts of its employees because Section 105 duties do not bear on employee motivation or whether the employee is acting within the scope of employment in connection with the underlying criminal act. As the Commission notes, 18 U.S.C. § 2520, paragraph (a), already provides civil remedies for persons whose wire, oral, or electronic communications are intercepted, disclosed, or intentionally used in violation of Title III. In such a civil action, the person may recover from the "person or entity" which engaged in the violation. 18 U.S.C. § 2520(a).

Law Enforcement believes that the duties assigned to carriers under Section 105 would not expand the potential for such liability because, under common law principles, employers are already required to act reasonably in hiring employees and in supervising their activities. Compliance by a carrier with the regulations implementing Section 105 evidences that the carrier acted reasonably and mitigates against imposing vicarious liability for the intentional act of its employee; if carriers fail to comply with the regulations, such

Law enforcement is charged with the responsibility of protecting citizens against illegal invasions of privacy, including by carrier personnel. Illegal intercepts or disclosures of electronic surveillance could conceivably occur during the implementation and maintenance of a lawfully authorized intercept as a result of the improper or negligent conduct of carrier personnel. Appropriate carrier personnel policies and procedures are required, therefore, in order to protect the respective interests of the carrier, law enforcement, and the public.

38. Initially, carriers should be required to establish a "vetting" process for carrier personnel designated and authorized by the carrier to receive and implement intercept orders, or certifications, or who otherwise have access to electronic surveillance activity and information. While a carrier's normal hiring and other personnel processes would likely include some inquiry into the credit and criminal histories of any prospective employee, the Commission's rules should include carrier policies and procedures that recognize that those select employees who are designated to effect electronic surveillance should be of demonstrable trustworthiness. Hence, carrier policies and procedures should include a background check commensurate with the sensitivity of the activities in which the designated employee will be engaged. The Commission should be aware that such trustworthiness determinations and background checks are consistent with the existing practice of carriers with regard to security personnel who today handle and administrate electronic surveillance orders.

39. The Commission should specify that this information should be collected and included in individual records for all designated personnel who participate in intercepts or have access to electronic surveillance information. Policies of this sort not only help law enforcement in the event an intercept is compromised or electronic surveillance information is improperly disclosed, they should afford protection for the carrier in making personnel

noncompliance will be evidence of negligence, and will tend towards imposition of vicarious liability. Thus, to the extent a carrier is exposed to possible derivative liability under *respondeat superior* or a claim of negligence, the risk of exposure will be substantially mitigated, if not eliminated, by compliance with CALEA.

assignments to security functions, and demonstrate that reasonable steps have been taken.

40. To the extent that carriers become aware of information regarding any security personnel that would call the integrity of a particular designated employee into question, carriers should be required to take immediate steps outside the normal personnel review process to reassign that particular individual pending more thorough review. In addition, security personnel should be required to execute nondisclosure agreements, the terms of which would survive the employee's reassignment or departure from the company, that also certify that the employee has been apprised of the criminal and civil penalties applicable to the improper disclosure of surveillance-related information. These agreements should remain with the employee's permanent records.

41. In addition to law enforcement's security interest in these procedures, it likewise is in a carrier's interest that these agreements be obtained and that related procedures be clearly stated and assiduously pursued. For example, in the event that claims are made against a carrier arising from an alleged illegal intercept or the unauthorized disclosure of electronic surveillance information, the existence of clear and specific policies and procedures and demonstrable evidence that they were followed in a particular case should provide the carrier with a defense to an action based on its non-negligent, good faith conduct. As noted above, the foregoing policies and procedures safeguard the interests of all concerned - - the carrier, law enforcement, and the public.

2. Reports of Violations.

42. Law Enforcement believes it is important for a carrier's duty to include the affirmative obligation to report violations of its security policies and procedures and compromises, or suspected compromises, of intercepts. Thus, in the event a carrier acquires information that leads it to suspect that its employee may have engaged in illegal surveillance activity on his own, that information should immediately be reported to the FBI or the cognizant law enforcement agency for further investigation. At a minimum, it also is

presumed that the employee would immediately be reassigned pending the outcome of the investigation. It is understood that this practice has historically been followed by carriers.

43. Law Enforcement also strongly agrees with the Commission's suggestion in Paragraph 27 of the NPRM that carriers should be required to report any compromise, or suspected compromise, concerning the existence of an interception to the affected law enforcement agency, or agencies. Indeed, because of the potential threat to the safety of witnesses, undercover agents, and intercept subjects that a compromise could represent, carrier technical personnel should be required to report such compromises, or suspected compromises, to the carrier security office immediately upon discovery. At a minimum, the Commission should require that no more than 2 hours be allowed to elapse between the discovery that an intercept has been compromised, or is suspected of being compromised, and the report of that fact to the affected law enforcement agency or agencies.

44. The standard that should apply in determining whether an intercept may have been compromised should be the standard of reasonable suspicion. In this regard, carrier personnel should be required to report objective facts that would reasonably give rise to the suspicion that an intercept had been compromised. Upon discovery of such facts, carrier personnel should be required to report the suspected compromise to the security office, which, in turn, would report it to the law enforcement agency involved. The Commission should develop a standard for determining what preventative measures would reasonably be required to ensure that compromised intercepts do not go undiscovered or unreported. The existence of specific policies and the resulting demonstrable evidence should provide a carrier with a defense to an action based on its non-negligent good faith conduct.

45. Law Enforcement believes that reports of violations of carrier security policies and procedures and compromises of intercepts should be reported to the Commission on a regular basis. Such reports would enable the Commission to exercise more effectively its continuing jurisdiction over CALEA-related matters. But this reporting requirement should not be permitted to delay a carrier's obligation to immediately report to law enforcement